HACKER JOURNAL
n. 47
www.hackerjournal.it
QUATTORDICINALE ANNO 3/ 25 MARZO 2004 - 8 APRILE 2004 / SPED. IN ABB. POST. 70% - MILANO

I SEGRETI DEL CODICE NAZISTA

TELEFONATE NON PAGHIAMO PIÙ

LYX E SCRIVI DA SCIENZIATO!

9 771594 577001 40047
4ever

2€ NO PUBBLICITÀ SOLO INFORMAZIONI E ARTICOLI

ANTENNA WIRELESS FACCIAMOLA DA SOLI

POVERA MICROSOFT: VOLEVA BLINDARE XBOX

- WINDOWS XP: BASTA PROBLEMI
- SCACCO AL CAVALIERE BIANCO
- TUTTE LE FOTO IN RETE
- IL TETRIS PIÙ GRANDE DEL MONDO

HACKER JOURNAL

Anno 3 – N. 47
25 Marzo 2004 - 8 Aprile 2004

Direttore Responsabile: Luca Sprea

I Ragazzi della redazione europea:
grand@hackerjournal.it, Bismark.it, Il Coccia, Gualtiero Tronconi, Ana Esteban, Marco Bianchi, Edoardo Bracaglia, One4Bus, Barg the Gnoll, Amedeu Bruguès, Gregory Peron

Service: Cometa s.a.s.

DTP: Davide "Fo" Colombo

Graphic designer: Dopla Graphic S.r.l.
info@dopla.com

Copertina: Daniele Festa

Publishing company:
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing:
Roto 3

Distributore:
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81-
Tel. 06.33455.1 r.a.
20134 Milano, V.le Forlanini, 23
Tel. 02.75417.1 r.a.

Abbonamenti:
Staff S.r.l.
Via Bodoni, 24
20090 Buccinasco (MI)
Tel. 02.45.70.24.15
Fax 02.45.70.24.34
Lun. - Ven. 9,30/12,30 - 14,30/17,30
abbonamenti@staffonline.biz

Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

editoriale

Diamo spazio a Kasderton

Vorrei esporre il mio pensiero sul mondo hacker e sui futuri hacker del domani. Dando un'occhiata ai grandi della storia è possibile certamente affermare che gli hacker sono sempre esistiti: Pico della Mirandola ne è un esempio, come anche il grande Mozart (per citarne un paio), persone che, grazie alla forte volontà, curiosità, desiderio di apprendere tutto il possibile nell'ambito del proprio campo, hanno saputo addentrarsi in un mondo che è diventato di loro dominio. Ma anche ai giorni nostri, guardandomi attorno, vedo bambini curiosi che guardano tutto per cercare di capire, di imparare e penso che un domani continueranno a farlo ma non coi propri occhi, ma con quelli del fedele PC d'infanzia. Chiunque abbia appreso una conoscenza più che profonda in un ambito che lo appassiona può definirsi un hacker! Per quanto mi riguarda io sono cresciuto a pane ed MSX, apprendendo i rudimenti del Basic e realizzando a 10 anni i primi programmini in grado di produrre quelle allegre musichette o di tracciare poligoni e altre forme geometriche strambe. Con gli anni ho capito che il Basic era troppo riduttivo per i miei fini e, con grande curiosità e voglia di conoscere, ho iniziato ad avvicinarmi a linguaggi più adatti ai miei scopi. Eh sì, è proprio la curiosità il motore del mondo… e il mio ideale di hacker iniziava a delinearsi in maniera sempre più netta. Non sono di certo mancate le sfide e quelle che possono sembrare "astute truffe" ma in realtà per me non lo erano: era più il desiderio di riuscire a essere più furbi e intelligenti di qualcun altro! E allora via con i primi esperimenti per far alzare le sbarre di un centro commerciale con una tessera magnetica truccata, via con il social engineering per chiedere libri hacker troppo costosi mediante lettere di lamentele ben studiate, via con il tesserino della mensa opportunamente modificato, via con i primi programmini inviati a "poco svegli" utenti di mirc per cercare di dare un'occhiata al loro PC, via ai primi attacchi al server universitario, e così… via! Non è un'"istigazione a delinquere" ma semplicemente la volontà di sperimentare le proprie conoscenze, trucchetti usati una volta per soddisfazione personale e poi abbandonati per dignità e giustizia. Un vero hacker testa i propri studi ma non truffa il prossimo; sorride per l'incompetenza di persone che dovrebbero essere specialiste nell'ambito dell'informatica ma si rivelano alquanto incompetenti; ride però a crepapelle quando l'addetto delle poste cerca di far sparire la schermata blu sul proprio terminale con colpetti sul monitor sperando di ripristinare la sessione… chissà che sistema operativo è installato su quelle macchine! :-) Un hacker vuole sempre essere al centro dell'attenzione in ogni campo… e non sopporta essere spazzato via dal primo "garbage collector" di turno! E allora all'opera! E un consiglio: non mollate mai!
Un saluto generale.

Kasderton

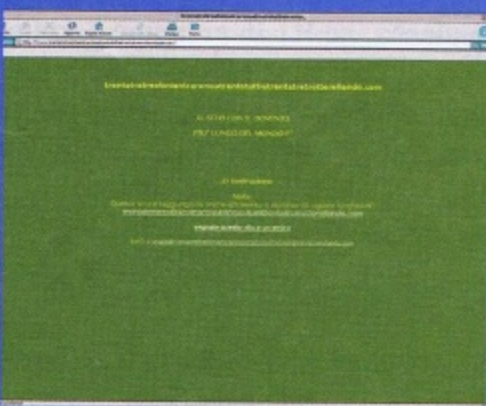
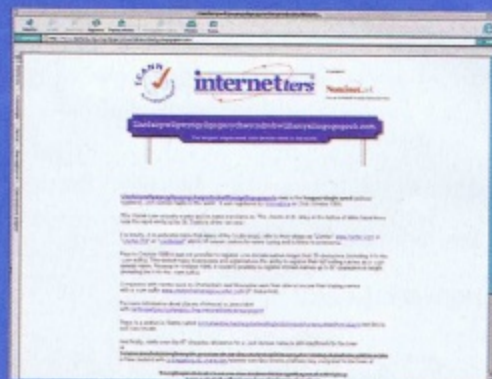
HACKER JOURNAL: INTASATE LE NOSTRE CASELLE
Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati. redazione@hackerjournal.it

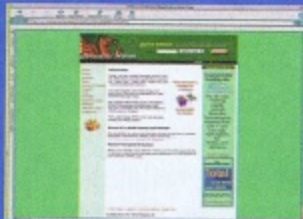
Ce l'ho LUNGHISSIMO!

Sulla rivista HJ45 avete pubblicato un articolo dove c'era scritto di trovare un dominio con il nome + lungo. Io ho trovato questo, cosa ne dite?
www.trentatretrentinientraronointrentotutti-trentatretrotterellando.com/

Albatro99

Ma non è solo Albatro99 ad averlo scoperto, http://www.trentatretrentinientraronoatrentotuttietrentatretrotterellando.com oppure della stessa lunghezzawww.trentatretrentinientraronointrentotuttitrentatretrotterellando.com"trentatretrentinientraronointrento-tuttitrentatretrotterellando.com provare per credere, esiste veramente.

C140 !!_TNK_!!

Ecco invece una soluzione ancora più assurda, ma vera:Volevate il nome di dominio più lungo: eccovelo :-)
http://www.llanfairpwllgwyngyllgogerychwyrndrobwyll-llantysiliogogogoch.com/
confermata da:

Con riferimento alla "sfida" lanciata da Hacker Journal 45 pag. 26 (in "La magia dei nomi risolti"), pare si tratti di: www.llanfairpwllgwyngyllgogerychwyrndrobwllllantysiliogogogoch.com/
Complimenti alla rivista!
frP.S.: come ho fatto? ricordavo che esiste una città col nome più lungo, col solito Google l'ho trovata, poi ho immaginato avesse un dominio...

...ma battuta, seppur di poco, da: Dns più lungo potrebbe essere questo?? www.llanfairpwllgwyngyllgogerychwyrndrobwllllantysiliogogogoch.co.uk

...e non è finita! Provate a interrogare via email qualche domain-registrar americano...

L'inno di Hacker Journal? Ma scriviamolo!!

Carissima e coolissima redazione,io sono un dj e ho un'ideuzza ke mi gira per la testa... voi ke ne direste se oltre ad avere un logo la nostra rivista preferita avesse anke un inno? Io avevo pensato ke le parole potessero essere scritte da tutti i lettori in collaborazione, e poi voi me le mandavate e io le avrei rappate, ke ne pensate?Spero l'idea vi piaccia!YO by DJ ZackCarissimo e coolissiimo DJ Zackci piace tantissimo e la lanciamo subito! Chi scrive le parole per l'inno rap di Hacker Journal?

SECRETZONE

Nuova Password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete gli arretrati, informazioni e approfondimenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo!

USER: H07A

PASS: T1PA

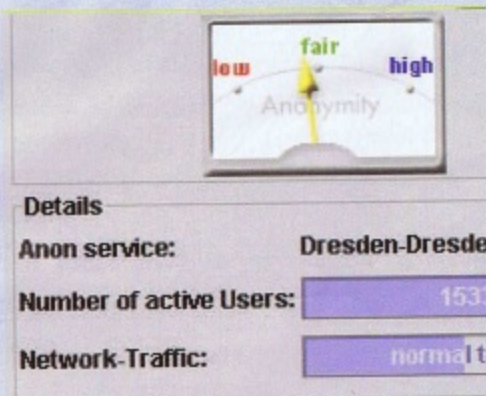
CARA ENEL, NON È COSÌ FACILE

Seguo sempre la vostra rivista e la trovo molto interessante. Volevo semplicemente segnalarvi che mi è stato cambiato il contatore Enel da poco con quello di nuova generazione e il contratto mi è stato mantenuto regolarmente alla mia solita tariffa, contraddicendo quello che si diceva nell'articolo riguardo un eventuale obbligo di cambio di contratto per la fornitura di energia elettrica e di passaggio a 3,3 kw. Probabilmente il caso dell'intervistato era davvero sfortunatamente particolare. Grazie cmq di esserci. Ciao

Volcano

Caro Volcano,
grazie a te. Forse hai interpretato male qualche frase dell'articolo, dove spieghiamo che ciò che si paga è il passaggio al contratto a 4,5 KW. A cui, ahimè, siamo spesso costretti per mantenere le stesse funzionalità che avevamo con i vecchi contatori, che sopportavano meglio i carichi usuali dei nostri elettrodomestici. L'intervistato sottolinea che non si capisce come mai, per avere quindi la stessa comodità di prima, ora ci troviamo quasi costretti a cambiare tipo di contratto. Per di più quando tale passaggio ai 4,5 KW è solo questione di settare un registro del nuovo contatore, variazione che ci fanno pagare la bellezza di 200 Euro a cui segue pure un canone più salato. Ma è proprio così giustificabile?

NASCONDERSI BENE

Raga mi serve un grosso aiuto su come usare un proxy per rendersi anonimi!!
Ho fatto ricerche varie in internet e ho trovato un programma di nome multiproxy e una sua guida per configurarlo!! Ho seguito attentamente la guida ma ho visto che non funzionava poi ho fatto un 'altra ricerca e ho trovato una cinquantina di siti sempre con la stessa guida!!
Non capisco, potreste spiegarmi come usare dei server proxy per rendersi anonimo?!
Vi prego aiutatemi.

Matteo

Ciao Matteo,
Vai a vedere il sito http://anon.inf.tu-dresden.de/ e scarica JAP, oppure, più comodamente, tieno d'occhio la nostra rivista cugina Hackers Magazine 17 che trovi pure lei in edicola, dove mettiamo sul CD proprio JAP, installabile immediatamente e con tanto di articolo che spiega come fare e come funziona. Ma torneremo presto anche su HJ su questo argomento parecchio attuale.

RICONOSCIMENTO DEL VOLTO: NON MI FUNZIONA!

Ho installato Alparysoft Videolock ma non funziona: quando lancio il software mi appare il messaggio "Can't connect detector. Try to reinstall Alparysoft Video Lock". Spero che possiate aiutarmi grazie.

Matte

Ciao Matte!
Credo che la risposta tu l'abbia sotto gli occhi: reinstalla il software, magari scaricandolo nuovamente dal sito o dal CD della nostra rivista cugina Hackers Magazine n°16 di Marzo. Ma prima di tutto controlla che con qualunque altro sistema la tua webcam funzioni bene e sia installata correttamente (se usi Windows XP puoi vederlo direttamente dalle risorse del computer, facendo due clic sul nome della webcam). Vedrai che funzionerà al primo colpo! Per chi si fosse perso qualcosa: su HJ 45 abbiamo parlato a pagina dieci di come ingannare il sistema di riconoscimento facciale che troviamo scaricabile anche al sito http://www.alparysoft.com/.

BELLO E SI VEDE!

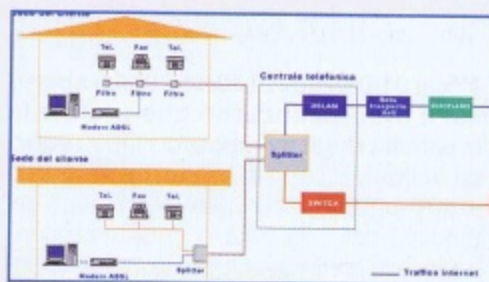
Vi seguo da qualche numero e trovo la rivista molto interessante (anche se non è che sia un programmatore

eccelso). Ecco, vorrei segnalare il sito www.viaoberdan.it. C'è una cosa: è un sito che parla di letteratura. Sono fuori tema? Beh, il sito esiste dal 2000 e inizialmente veniva sviluppato con i programmi di Zio Bill. Ora l'abbiamo ricostruito lavorando su piattaforma linux con software libero. È stato un lavoraccio! Adesso, se fosse possibile farlo sapere a tutti coloro che come noi apprezzano il pinguino... sarebbe una soddisfazione e un premio alla nostra fatica! L'hacker che tra un codice e un altro avesse voglia di leggere un racconto o una poesia... sarà il benvenuto :-) Ciao

Thomas

Dobbiamo dire che ci pare proprio un bel lavoro, anche se un po' diverso dai nostri temi abituali. Quindi lo segnaliamo volentieri, invitando i 'letterati' a dargli sicuramente un'occhiata e tutti gli altri a prendere spunto per qualche idea da copiare (chiedendo autorizzazione!) sul proprio sito. Ma chi l'ha detto, poi, che tra hacker non ci sia la sana curiosità per la letteratura?

... E PER BEFFARE L'ADSL?

Ciao a tutti! Premetto di non intendermi di computer (una vita fa avevo un Commodore Plus4, passavo ore su ore a fare listati in Basic che chissà perché non producevano nulla), uso Windows Xp (per comodità, Microsoft mica mi sta poi tanto simpatica...) con un modem 56k e il mio primo Pc l'ho acquistato l'anno scorso. Dopo aver letto l'articolo "Enel beffata",m'è sorta spontanea la domanda <<Sarà possibile fregare anche Telecom ?>>. Cioè, esisterà il modo di connettere un modem adsl senza pagarne il relativo canone? Non so come funziona l'adsl ma mi pare che fino a una certa "quota" di kbit per fare l'allacciamento non è necessario alcun tecnico, per cui i cavi del telefono non dovrebbero cambiare. Forse alla Telecom sono meno sprovveduti che all'Enel e avranno tutte le contromisure, però m'interesserebbe saperlo a livello teorico. Sottolineo che anche se il modo esistesse, sarei il primo a sconsigliarne l'uso: non vale la pena di certo andare in galera per avere un po' di banda in più risparmiando i 40 euro al mese di un abbonamento flat!

Drago

No, non è possibile perché le premesse sono sbagliate. Immagina la linea telefonica come un tubo pieno d'acqua a cui, quando e solo quando si chiede di far passare i dati nella modalità offerta dalla tecnologia aDSL (Asymmetric Digital Subscriber Line), viene aggiunto dell'olio. A casa tua un filtro (il filtro o lo splitter aDSL) montato sul normale doppino telefonico (i due fili che ti arrivano in casa) separa l'acqua dall'olio: l'acqua verso i telefoni, l'olio verso il modem. Tutto qui. Se nessuno attacca il tuo doppino in centrale anche al modem aDSL corrispondente, l'olio non ti arriverà mai: solo acqua. Quindi nessuna 'quota' o 'extraquota' possibile. Differente è il caso di quei fornitori che fanno funzionare il telefono e il modem in tecnologia digitale sfruttando il doppino solo per aDSL, tramite cui passano anche le telefonate. Per rimanere nell'analogia: tutto diventa olio (pacchetti di dati), anche ciò che prima era acqua (segnale analogico). È quanto fa Fastweb e qualche altro. Allora lì la velocità della linea può arrivare fino a 4 MB, solo se i collegamenti fisici alla centrale sono corti (devi essere vicino alla centrale) e se sono perfetti (non devono passare su cavi vecchi o centraline usurate). Ma queste condizioni sono accertabili solo da un tecnico che stressi la linea fino a capire se sopporta i 4 MB. Se sì, apre il rubinetto. Se no, lo tiene regolato per farti avere 'solamente' 2MB, che invece possono passare su linee distanti e vecchie.

DEDICATA A TUTTI

*Cara redazione di HJ,
eccovi una poesia dedicata agli hacker.*

Hacker
Estensione scomponimi
non zipparmi
perchè dell'uomo non si può sminuire l'essenza.
Acquisisci tra le porte la mia sapienza.
In esadecimale sognami
perché di tutto ciò sono il compositore.

Dopo questa poesia volevo farvi una richiesta, perché non pubblicate un articolo sul lock picking o sul phreaking?? Saluti

Blackhole #0

**Ottimo, Blackhole#0 !
Ci è piaciuta e come vedi la pubblichiamo. In cambio un po' di pazienza: hai toccato due argomenti che sono nel cassetto dei lavori in sospeso. Se qualche lettore vuole contribuire ad accelerarne l'uscita, ci mandi le sue esperienze, stiamo raccogliendo il materiale utile!**

HOT!

LA BEFFA DEL CELLULARE RUBATO

Alcatel, Motorola, Nec, Nokia, Panasonic, Sagem, Siemens e SonyEricsson si sono impegnate a creare un unico database globale di IMEI (Central Equipment Identity Register, CEIR), il numero che identifica univocamente ogni cellulare, per mettere automaticamente fuori uso i cellulari rubati. Peccato che basti riprogrammare l'IMEI o, più semplicemente, utilizzare il cellulare rubato in Paesi che non supportano il sistema basato sugli IMEI, per sfuggire al blocco. Non a caso i cellulari rubati in Europa occidentale finiscono spesso in Africa o in Europa orientale, dove il sistema basato sugli IMEI non è utilizzato. I produttori di cellulari hanno comunque accolto un invito della GSM Association per migliorare la sicurezza dell'IMEI e hanno annunciato l'intenzione di implementare su tutti i nuovi cellulari una tecnologia che blocchi a livello globale un telefonino rubato.

TIM, EDGE E UMTS: GULP!

Sta arrivando alla grande anche la tecnologia EDGE su rete GSM, che si avvicina, come prestazioni, a quella UMTS. EDGE incrementa la velocità della GSM dai 38 kbps attuali del GPRS ai 200 Kbps, più della metà dei 384 Kbps dell'UMTS, che poi nella pratica sono mediamente 22 kbps per il GPRS a 150 mila per EDGE, contro i circa 230 mila di UMTS. TIM lancerà EDGE su vasta scala già in aprile e per giugno, preparandosi per il successivo boom di Natale, offrirà UMTS e relativi videotelefonini.

SOLDI CON OPENSOURCE!

Dal 01/03/2004 al 30/11/2004 è aperto il primo concorso che premia la creatività degli sviluppatori OpenSource italiani. Riservato ai privati realizzatori di un progetto Open Source connotato dal requisito dell'originalità, e rilasciato secondo licenze certificate OSI (http://www.opensource.org) si sviluppa in diversi filoni, ciascuno dei quali prevede premi in denaro e… tanta fama! Ad oggi i progetti in gara sono 18. Aumentateli! Ecco in breve, dal sito http://www.opensourcecontest.it/ le categorie a cui ci si può iscrivere:

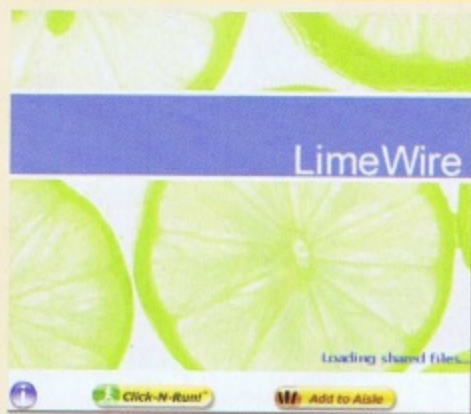
- **Innovazione** - Never done before
Il software più "particolare" e "innovativo" - 1.500 € al vincitore.
- **Miglior Interazione Utente** - User friendly Power
L'importante, questa volta, è l'interazione con chi sta davanti al monitor - 1.500 € al vincitore.
- **Best Community** - Cooperative knowledge
Documentazione, aiuto ai nuovi utenti, forum, chat, mailing list: verrà premiato il miglior supporto agli sviluppatori ma anche, e soprattutto, ai semplici utilizzatori - 1.500 € al vincitore.
- **Sicurezza, Networking, Comunicazione** - Follow the [white, black, gray] hat... Tra software anti-cracker, monitor di rete, tool di gestione remota, e qualsiasi altro lavoro che metta ordine tra flussi più o meno disordinati di informazioni, ci sarà un solo vincitore - 1.500 € al vincitore.
- **Multimedia (Grafica, Audio, Video)** - It [sounds, looks] wonderful
Non potendo premiare gli artisti, premiamo gli strumenti migliori - 1.500 € al vincitore.
- **Business (Database, Office, System Integration)** - This is not a joke!
Vinca il migliore - 1.500 € al vincitore.
- **Tesine scolastiche (Università, Scuole superiori)** Perché tutto questo lavoro non venga ignorato - Quattro premi per questa categoria: il primo da 400 €, il secondo da 300 €, il terzo da 200 € e il quarto da 100 €.

Open Source Contest 2004 — 1° EDIZIONE

1 MILIONE DI DOLLARI PER 10 ORE DI DESERTO

Venticinque partecipanti per la sfida lanciata dal Pentagono: costruire un veicolo capace di attraversare il deserto da Barstow, in California, fino a raggiungere un'area vicina a Las Vegas, in dieci ore e senza l'aiuto umano. Il primo che arriva vince 1 milione di dollari. Il veicolo, di qualunque forma o dimensione, deve superare ostacoli impensabili, tra cui ferrovie, rocce, dune, strade e quanto altro, oltre a riuscire a sopravvivere a condizioni metereologiche estreme. Non conosciamo ancora il vincitore, ma vi sapremo dire se qualcuno c'è riuscito e come è andata a finire. Anche perché i team che hanno partecipato hanno inserito nei loro veicoli tecnologie di tutto rispetto, soprattutto per quanto riguarda il riconoscimento degli ostacoli e il posizionamento con avanzati sistemi GPS.

P2P FINALMENTE LIBERO IN EUROPA!

A larga maggioranza il Parlamento Europeo dà il via libera allo scambio dei file via P2P tra privati. Con l'eccezione e inasprendo le già pesanti sanzioni per chi ne fa un uso commerciale e distribuisce illegalmente cd e dvd. L'articolo è un po' subdolo perché recita qiualcosa come "si dovrebbe tenere conto degli interessi dei terzi inclusi, segnatamente i consumatori ed i privati che agiscono in buona fede". Ma nel resoconto dell'ufficio stampa dell'Europarlamento si legge "Significa che gli atti commessi in buona fede dai consumatori - come lo scaricare musica da Internet a uso personale - non saranno perseguibili".
Era ora! Così, mentre negli Stati Uniti si viaggia ancora con la mano pesante e continuano le denunce da parte delle case discografiche a privati che usano software P2P, in Europa si conferma una visione che tiene conto di quella che è ormai una realtà: la musica tra privati si ascolta per scambio libero. Contro i pirati di professione, l'Unione Europea è comunque molto più rigida perfino degli USA: le vittime di violazioni del copyright potranno richiedere persino il congelamento dei conti correnti bancari dei pirati oltre alle procedure penali eventualmente previste dai singoli stati membri, che restano valide. La direttiva deve ancora passare al Consiglio dei ministri dell'Unione, che prevede di adottarla in maniera definitiva entro l'estate. Dopodiché, i governi dei singoli stati avranno 24 mesi di tempo per la ratifica.

COMPUTING ALTERNATIVO E AMIGAONE

Il portale IkSNet e tutti i siti del circuito sono ospitati su un server AmigaOne G3-SE. Il server è finanziato da Alternative-Technology e la gestione tecnica è affidata a Soft3. Nuove iniziative sono previste a breve e, come dicono i gestori: "siete tutti invitati a visitare www.iksnet.it e provare il nuovo server". Ci suggeriscono dalla regia: la linea potrebbe esser sovraccaricata a causa della mole di accessi causati da questo annuncio.

SCENEGGIATI E MOLTO ALTRO, GRATIS

www.the-jackal.net

Il sito parla di Pc, Giochi, Console, Cinema, Musica e molto altro. Nella sezione download si possono trovare da una miriade di programmi per la xbox, ps2, pc agli sceneggiati di film famosi, il tutto gratuitamente. Nel sito sono presenti news, trucchi per le console xbox, ps2, GameCube e presto anche quelli per PC. Abbiamo il forum, con uno staff pronto a risolvere qualsiasi problema si riscontri con il pc, con la xbox, con la ps2 e con il gamecube. Insomma, un sito con un po' di tutto.

HOT!

WEB GRATIS AI VOLONTARI!

Gabama.com è un servizio completo di hosting web offerto gratuitamente alle associazioni certificate come ONLUS, cioè "Organizzazione Non Lucrativa di Utilità Sociale". In pratica tutte le associazioni di assistenza, soccorso, tutela della natura, organizzazioni umanitarie e simili non dovranno più pagare per la loro presenza sulla Rete. La qualità dei servizi offerti è paragonabile e forse superiore a quella proposta da analoghi servizi a pagamento. Non è richiesto l'inserimento di banner o altri elementi pubblicitari: lo spazio offerto è completamente a nostra disposizione. Il sito costruito sarà gestibile tramite un pannello di controllo che ci permetterà d'installare diversi software gratuiti. Gabama.com offre gratuitamente anche l'assistenza completa alla gestione: non occorre essere esperti webmaster.

SONO HACKER OPPURE...

Hanno defacciato il sito di http://amsn.sourceforge.net/ che fa parte del progetto sourceforge.org. Ma possiamo ancora definirli hacker? Ecco il commento degli amministratori del sito stesso:
"Siamo spiacenti di comunicare che il sito AMSN è stato hackerato oggi. Abbiamo quindi perso alcuni nuovi messaggi.
Ciò dimostra come ci sono prsone ch si divertono a rendere il nostro lavoro più difficile. Noi spendiamo un sacco di tempo a scrivere su amsn, e ora dovremo trovare il tempo di preoccuparci della sicurezza del sito e delle politiche di backup. Grazie molte a questa gente. Questo gruppodi "hacker?" (noi pensavamo che gli hacker non fossero come questi, chiamiamoli "script kiddies") ci hanno dato un contatto email: pcdelisi@hacker.am
Il Team AMSN"

LO SCACCO

Dicembre 1991: un esperto francese di sistemi Unix e di reti viene trasferito in Svezia per lavorare come ingegnere addetto ai computer. La città è tra le più squallide: Flen. Otto non riesce a vivere una vita sociale adeguata non certo per sua colpa. L'hacking rimane l'unico motivo per trascorrere le giornate! Iniziano lunghi viaggi in Synchron City, una BBS molto famosa, e dentro QSD, la ""mecca"' degli hacker. Otto decide così di allacciarsi a Datapak, un network diffuso in Svezia per la conveniente offerta proposta, che gestendo pochi abbonamenti aveva un efficiente servizio di monitoring: chi abusava del servizio poteva essere subito rintracciato... Attivato il collegamento a Datapak mancava a Otto uno username e una password. Per ottenerli ha un flash: scandire il network alla ricerca di NUI (Network User Identifier) validi, cioè di identificativi utente. Otto costruisce così il suo NUI Scanning che funziona piuttosto bene e riesce con estrema sorpresa a trovare quasi subito un NUI e una password validi.

Verrà poi appurato che si trattava di un abbonamento test, una dimenticanza della Televerket, la società di comunicazioni che gestisce Datapak. Otto può finalmente entrare in QSD e chattare con i suoi amici.

L'incontro con White Knight

Ottobre 1992. Otto viene contattato da un misterioso White Knight.

Le discussioni vertono prima su alcune questioni di hacking, ma presto virano bruscamente verso tematiche più piccanti. Otto gli rivela, forse ingenuamente, ciò che egli stesso aveva fatto: scanning per rubare NUI e password allo scopo di addebitare i costi della propria con-

RedIRIS - Workshop of Abuse Teams Program information
Madrid, Spain 14th January 2004

Preliminary Program

▲ Pege Gustafsson è sempre uno stimato professionista dell'ex Televerket, ora Telia, che spesso possiamo incontrare in seminari dedicati alla sicurezza aziendale.

DEL CAVALIERE BIANCO

Annoiato della cittadina svedese in cui vive, Otto Sync si dedica all'hacking. White Knight responsabile di sicurezza informatica, è tradito da paranoie. Una partita avvincente. Ma lo scacco è matto...

nessione ad altri utenti regolarmente iscritti. In altre parole: abuso di servizi informatici! Le discussioni procedono per giorni con White Knight che registra e stampa ogni parola e ogni connessione del nostro amico.
Otto è naturalmente ignaro di tutto ciò. White Knight ha disposto bene le sue pedine. Continua a giocare a lungo fino a che arriva il momento tanto desiderato: vuole lo scacco e lo vuole matto. Il "'cavaliere bianco"', un vero professionista in giacca e cravatta della Televerket, impegnato in questa operazione di ricerca dell'hacker, prepara il blitz.
Il 2 dicembre Otto apre la porta del suo ufficio e riceve una visita di un certo Pege Gustafsson. Gustafsson non è altri che White Knight con tanto di mandato di arresto e polizia svedese alle spalle. A Otto pare di svenire, ma non si dà per vinto. Viene perquisito l'ufficio e anche la casa di Otto, che davvero non si aspettava questo epilogo.
Ma la partita non era ancora chiusa.

L'interrogatorio

Pege Gustafsson non ha intenzione di mollare la presa e Otto non vuole certo cedere alle accuse legali. Tutto l'interrogatorio si basa su questo gioco psicologico che Otto vince con un certo vantaggio. Gustafsson ha sì in mano tutti i tabulati delle connessioni di Otto e in più la trascrizione fedele di tutte le loro chat su QSD. E l'accusa è anche semplice: Otto ha abusato di servizi informatici, scandendo il network e collegandosi con abbonamenti rubati! Otto era cosciente di ciò che faceva, ovvero operazioni di hacking, ma appoggiato da un avvocato che lo stesso Otto dirà "'essere professionale, capace e interessato al caso"', risponde che ha trovato l'abbonamento test e lo ha utilizzato pensandolo come un reverse-charge, cioè come un numero verde. Poi è entrato in QSD con la volontà di chattare con amici. Tutto qui!
E' andata davvero così? Davvero era questo l'intento di Otto? Certo che no, ma l'accusa non saprà costringerlo a rivelare la verità. Otto mantiene una posizione di innocenza e quasi di ingenuità rispetto a ciò che gli imputavano. L'avvocato provvedeva a rabbonire la tensione dell'interrogatorio con un ricamo di eloquenza e retorica. Un'accoppiata di tutto rispetto che frastorna i giudici. Dopo l'interrogatorio Otto viene accompagnato in carcere. Pochi giorni dopo si è svolto il processo preliminare che ha mantenuto gli stessi toni. La corte decide di non proseguire con lo stato di detenzione, ma opta per un "'travel ban"', cioè la requisizione del passaporto e l'obbligo di presentarsi ogni sera alla stazione di polizia. Un buon segno, e un paradiso per quella che invece poteva essere una pena davvero massacrante.

L'indagine secondo Gustafsson

Il responsabile della security, Gustafsson, racconta in seguito com'era nata l'indagine. Era dal 1990 che l'azienda stava allerta, quando due fratelli dell'8LGM – gruppo hacker all'epoca famoso – riuscirono a penetrare in Datapak creando notevole scompiglio. E' allora che crebbe a dismisura la paura per attacchi informatici. Ebbene, quando il nostro White

Knight incontrò Otto non ci mise molto a collegare tale paura al suo istinto di investigatore. Forse esagerando, visto col senno di poi.

Otto di fronte alla corte

Al processo preliminare è quindi seguita l'udienza vera e propria. Pege Gustafsson venne estraniato dall'aula in quanto la sua presenza non era più giustificabile: una prova dell'abilità dell'avvocato di Otto. Senza l'esperto, sia la corte che la giuria e perfino i più alti rappresentanti della Televerket non avevano le giuste competenze per capire veramente ciò che Otto aveva combinato. Otto, quasi divertito, riuscì a far girare a suo favore ogni accusa ammorbidendo i toni dello scontro con la sua presunta ingenuità. Tutto il materiale presentato dall'accusa parve così senza fondamento e Otto apparentemente si salvò. Non così la sua immagine, però, che da quel momento fu considerata una figura oscura, pericolosa, appartenente a una "'cerchia deviata"' di informatici. Il solito polpettone di accuse che vengono associate tutt'ora a tutti coloro che si definiscono hacker.

La sentenza

"'Non colpevole"'. Scacco matto di Otto, che nonostante sia realmente colpevole esce illeso da un processo anomalo.

PROVE SCHIACCIANTI?

OttoSync : The previous [NUI I used] was 159800. Are you from Sweden by the way?
WightNight : Sweden what.
OS : Just wondering... If you don't want to chat, then why go on QSD?
WN : Of course I want 2 chat. I'm Swede! R U?
OS : Nope I'm French. But I like Televerket, except when they send me bills :)
WN : Do they? Why?
OS : I asked for a NUI some weeks ago to get the technical doc about the PAD... But I won't pay!

▲ *Uno dei tabulati portati al processo come prova d'accusa verso Otto, che dopo avere inventato il suo scanner usava NUI sempre diverse*

Oggi, quell'Otto Sync annoiato che in quel di Flen ha praticato l'hacking, a spese della Televerket, è il responsabile di una società di IT Security asiatica. Quasi viene voglia..., ma è necessario saper giocare bene. A scacchi.

(liberamente tratto da Copyright Does Not Exist e adattato da Alone Sparrow)

COME A FATTO OTTO

Datapak è una rete packet-switching X.25 nata negli anni '80, dove gli utenti condividono poche linee dedicate e pagano in base alla quantità di dati trasmessi. Funziona chiamando un pop di accesso a numero verde. Quindi si digita il numero identificativo (NUA) di un computer perennemente collegato alla rete e una password utente. La rete è utilizzata per interconnettere analoghe reti di altri paesi, come TymNet (USA), SprintNet (USA), Telepac (Francia), Itapac (Italia), eccetera. Ogni paese ha anche un proprio identificativo di rete (prefisso, DNIC), il quale va anteposto al NUA per chiamare un paese differente.
Otto iniziò a provare i codici di accesso alla rete, come fece prima di lui il gruppo inglese 8LGM che effettuò una serie di scanning su 22.000 indirizzi X.25 Datapak, violando 380 sistemi informatici in tutto il paese. Scoprì anche, leggendo un manuale di Datapak, che collegandosi al numero verde e fornendo il proprio identificativo di rete (NUI) si potevano effettuare tutte le chiamate X.25 che si voleva e il traffico dati sarebbe stato addebitato alla NUI utilizzata. Il manuale forniva anche una serie di informazioni utili, con frasi del tipo:
"'Quando il modem risponde, digitate tre volte punto seguito da un invio, poi inserite:
N123456XYZ123-024037131270 <CR>
dove N indica al PAD con il quale siete connessi che quanto segue sono l'utente e la password (utente+password=NUI) mentre 123456 e' l'identificativo (utente) che vi assegnano nel momento della sottoscrizione all'abbonamento Datapak e XYZ123 è la vostra password.
Il numero dopo il trattino "'-"' è l'identificativo di rete (NUA) che volete chiamare (il computer al quale volete collegarvi)"'.

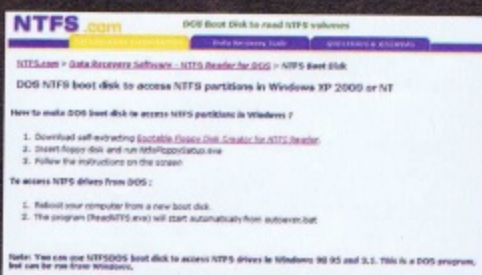
▲ *Flen, lo sperduto posto senza amici che ha consentito a Otto di starsene intere nottate attaccato al pc*

"Windows Recovery"

ATTAKKO BRUTALE alle password di Xp

Ecco un trucco che funziona se abbiamo installato Windows XP su una macchina che aveva Windows 98. Il vecchio sistema operativo deve essere ancora presente su un'altra partizione del disco. Abbiamo dimenticato la password di Amministratore di Windows XP e possiamo far partire il pc solamente da Windows 98. Come facciamo a recuperare la password dimenticata?

Gli strumenti indispensabili

Accendiamo la macchina e andiamo sotto Win 98. Tramite il nostro browser visitiamo il sito http://www.ntfs.com/boot-disk.htm

e scarichiamo il file Bootable Floppy Disk Creator for NTFS Reader.

Poi spostiamoci sul sito http://www.insidepro.com/download/saminside.zip e scarichiamo SAMInside, un 'cacciatore' di password, e memorizziamo anche questo sul nostro disco rigido. Riprendiamo NtfsFloppySetup.exe. Due clic su questo file .exe e inseriamo un dischetto. Un clic su Start e dopo un minuto il floppy è pronto.

Passo per passo

Riavviamo il pc con il dischetto dentro il driver e passiamo al Bios. Indichiamo come disco di avvio il floppy drive, salviamo e usciamo. Pochi giri del dischetto e appare la scritta:

"Select the software you want to use"

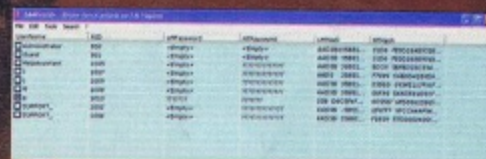
Rispondiamo con la voce 0, ovvero "Ntfs reader for dos". Cerchiamo l'unità su cui è installato il nostro Windows XP in panne e usando le frecce da tastiera arriviamo a:

```
C:\Windows\system32\config
```

dove c'è il file

```
SAM
```

Selezioniamolo, Ctrl+C per copiarlo e scriviamo la path di salvataggio che raggiunge la partizione su cui è installato Windows 98.

Copiamo anche il file System con lo stesso metodo, dalla stessa cartella. Avviamo Win 98 e diamo un occhio al tutto per vedere che i file SAM e System siano davvero stati copiati.

Recuperiamo saminside.zip, scompattiamolo e un clic sul file SAMInside_ Demo.exe. Nel menu File -> Import SAM diciamogli dove abbiamo messo il file SAM copiato. Poi diciamogli anche dove abbiamo messo il file System copiato (ce lo chiede lui). Un clic su Search e poi su Start on LM Hashes (F5). Attenzione: la versione demo che stiamo utilizzando riconosce solamente password scritte in lettere maiuscole, ma in caso di assoluta necessità la versione full la possiamo acquistare per soli 40$.

Dovremmo esserci! Se tutto va bene. ■

AUTOPSIA

Microsoft vuole che la Xbox sia una console chiusa. NOI NO!

La cosa più difficile da fare per modificare l'interno di una Xbox è... aprirla. Ecco come si fa. Seguendo queste istruzioni, si arriva a smontare completamente una Xbox.

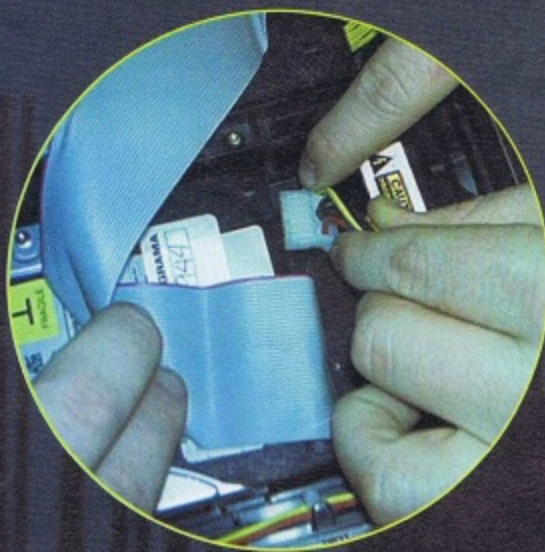
Primo: togliamo i piedini di gomma e gli adesivi.

Secondo: svitiamo le viti che stanno sotto i piedini. Serve un cacciavite Torx 20.

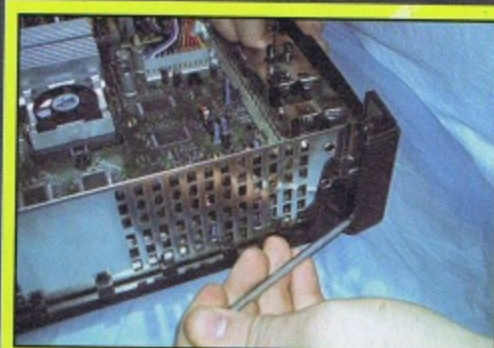
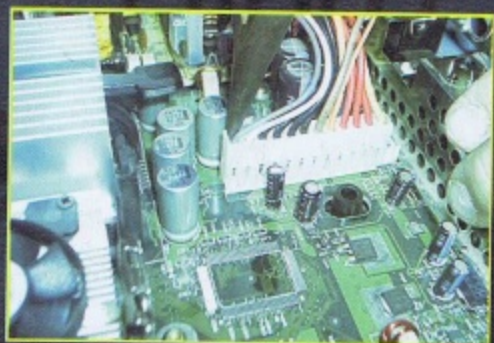
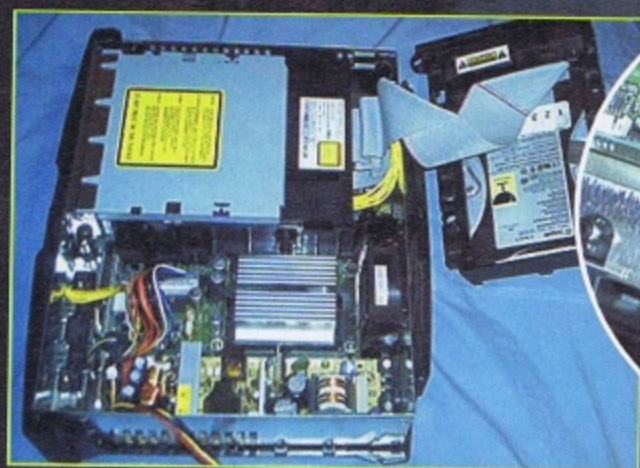
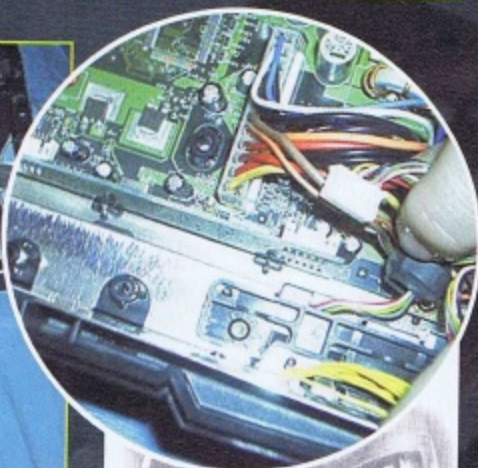
Terzo: svitiamo la vite che sta sotto l'adesivo bianco con il codice a barre.

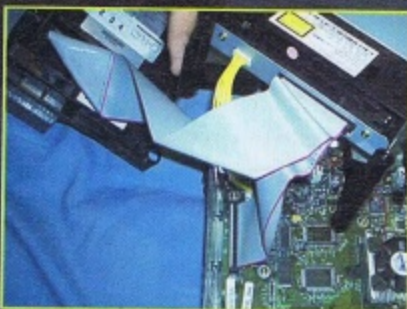
Quarto: svitiamo la vite situata sotto l'adesivo, diciamo, di presentazione. Serve il cacciavite Torx 20.

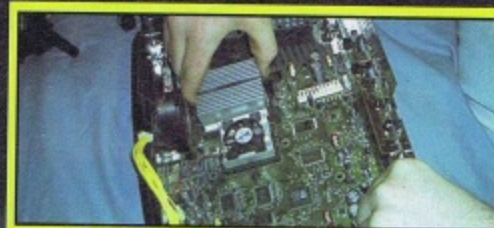
Quinto: capovolgiamo la Xbox e leviamo la parte superiore del case.

di una XBOX

Sesto: togliamo la corrente al disco rigido staccando il cavo di alimentazione.

Nono: stacchiamo il cavo IDE dalla scheda madre.

Decimo: sconnettiamo il cavo on/off dalla scheda madre. Dovrebbe essere composto da più cavi gialli, vicini al frontale della Xbox.

Tredicesimo: rimuoviamo il frontale. Ci sono due clip frontali e tre clip interne, sulla schermatura metallica.

Quattordicesimo: scolleghiamo il cavo di alimentazione dalla scheda madre.

Settimo: svitiamo le viti che intelaiano l'hard disk alla console e liberiamo la struttura (telaio più hard disk). Serve il cacciavite Torx 10.

Undicesimo: scolleghiamo la scheda che controlla le porte.

Quindicesimo: tolte due viti, asportiamo la scheda di alimentazione.

Ottavo: ripetiamo esattamente la stessa operazione con il telaio del lettore CD, e stacchiamo i connettori sul retro prima di togliamo anche questo.

Dodicesimo: rimuoviamo quattro viti Torx 10 e smontiamo le porte del controller.

Sedicesimo: ci sono ben undici viti di mezzo, ma tolte quelle viene via anche la scheda madre.

WINDOWS XP BASTA

Usiamo la tastiera a schermo

Anche se non ci è capitato di rovesciare un bicchiere di Coca-Cola sulla tastiera, può capitare di aver bisogno di avere i tasti visibili a schermo. È una funzione che WinXp mette a disposizione degli utenti con difficoltà, ma la otteniamo anche tramite **Start ->Esegui -> osk**

Rimuoviamo componenti di Windows (Messenger compreso)

Non conviene farlo tanto se siamo alla ricerca di spazio, quanto invece se stiamo cercando di migliorare le prestazioni. I componenti di Win Xp, infatti non occupano tanto spazio ma, se non usati, appesantiscono comunque inutilmente il sistema.
Per rimuovere i componenti che vogliamo andiamo su **Start-> Pannello di controllo -> Installazione applicazioni ->Installazione componenti di Windows.**
Riduciamo ed eliminiamo i processi che partono all'avvio di Windows

Questo è un sistema molto importante per liberare memoria, per velocizzare le prestazioni generali di Windows e per ridurre il tempo di avvio. Un primo sistema consiste nell'accedere a MsConfig **(Start -> Esegui -> msconfig)**, poi clicchiamo su Avvio, spuntiamo le voci interessate e riavviamo. Se il nostro computer non è una scheggia in velocità ci ringrazierà se toglieremo i processi non strettamente necessari.
La stessa cosa la possiamo ottenere accedendo ai registri di configurazione **(Start ->Esegui ->regedit)** e cercando con Trova **(Ctrl+F)** le sottochiavi Run e RunOnce ch appariranno sotto HKLM\Software\Microsoft\Windows\CurrentVersion e HKCU\Software\Microsoft\Windows\CurrentVersion. A volte è necessario eliminare le chiavi per rendere effettiva la disabilitazione dell'avvio del programma.

Ripristiniamo Mostra Desktop

Mosta desktop è quell'iconcina con

```
[Shell]
Command=2
IconFile=explorer.exe,3
[Taskbar]
Command=ToggleDesktop
```

Sfruttiamo a fondo i segreti di Windows, esistono funzionalità nascoste e semplici trucchi per rendere Windows Xp più completo e più veloce

PROBLEMI

una matita che scrive su una lavagna azzurra e che permette con un solo clic di ridurre nella barra degli strumenti tutte le finestre aperte. Non è di solito molto considerata, ma se prendiamo l'abitudine di usarla si rivela piuttosto comoda
Creiamo il file ShowDesktop.scf con il Blocco Note (o il nostro editor preferito) e digitiamo in esso il seguente testo:

```
[Shell]
Command=2
IconFile=explorer.exe,3
[Taskbar]
Command=ToggleDesktop
```

Generiamo una nuova password

Dal prompt **(Start -> Esegui -> cmd)** scriviamo

```
net user nomeutente /random
```

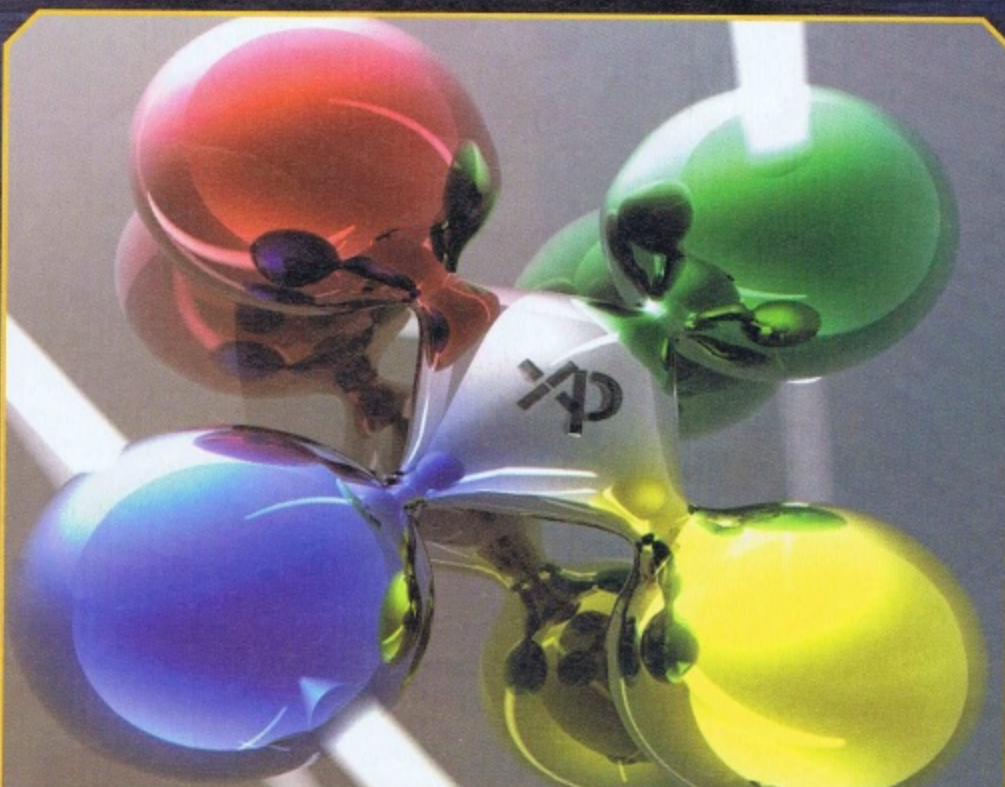
e verrà creata una stringa alfanumerica di 8 caratteri che, ATTENZIONE, verrà applicata automaticamente come password dell'utente corrente. Quindi prendiamone nota prima di proseguire!

Proteggiamo al massimo le nostre password

Dal prompt scriviamo

```
syskey
```

Nella finestra clicchiamo su Aggiorna. Possiamo scegliere tra 3 opzioni per proteggere le nostre pass con una chiave aggiuntiva (anche su floppy).
Attenzione, senza pass o dischetto non si potrà più accendere il computer! (non ci crediamo? okkio!...)

|void|
violet_room@libero.it

POMPA IL in AUTO

Con le centinaia di MP3 che abbiamo a disposizione, è un vero peccato non fare qualcosa per sentirli in macchina!

Un "problema" comune a molti è è il non poter ascoltare comodamente le proprie canzoni preferite, organizzate nel nostro iPod, mentre viaggiamo in auto. Le soluzioni possibili sono principalmente tre: iTrip, la finta musicassetta e un'interfaccia AUX. iTrip si è sempre rivelato interessante per l'idea, fosse solo per la comodità di non avere fili, ma in pratica si è dimostrato essere molto poco efficiente: difficoltà di sintonizzazione con la radio, brevissimo raggio d'azione e, non da poco, completamente inutile l'utilizzo in auto in Italia o in Europa a causa dell'altissimo numero di frequenze occupate.

La finta musicassetta è senz'altro una soluzione relativamente economica (circa 30 euro) e di facile utilizzo. Tuttavia se quello che cerchiamo è la qualità, certo non fa al caso nostro: fruscio di fondo insopportabile, rumorosità per il trascinamento, dispersione qualitativa elevata. Resta l'interfaccia AUX che, in base ai test che abbiamo effettuato, è senz'altro la soluzione migliore in relazione alla qualità audio di output ottenuta (l'aspetto per noi più importante). Tale interfaccia sfrutta l'ingresso digitale normalmente dedicato al collegamento del caricatore dei CD e lo rende un ingresso audio analogico, perfetto per l'uscita cuffie del nostro iPod.

Abbiamo trovato un'interfaccia AUX già pronta, da Bortesi (http://www.bortesi.it) e parleremo di essa, ma non è difficile con un minimo di intraprendenza fabbricarci in casa un apparecchio analogo. L'interfaccia AUX (AUX è l'acronimo utilizzato per la parola Auxiliar, che fa riferimento, nello specifico, a un ingresso supplementare di apparati audio e video e permette il collegamento di altri apparecchi).

▲ *L'interfaccia AUX è semplice. Da una parte il connettore per l'autoradio, dall'altra quelli per l'apparecchio da collegare. In mezzo la circuiteria di conversione del segnale.*

VOLUME con iPod

È essenzialmente costituita dal nucleo centrale (il convertitore analogico-digitale), il blocchetto d'inserimento per l'autoradio (che differirà in base al modello in nostro possesso) e i due classici connettori analogici RCA, ai quali collegheremo un cavetto RCA->minijack da 3,5 mm che porterà il segnale dall'iPod all'interfaccia.
Come prima operazione dovremo smontare l'autoradio (nel nostro tutorial siamo intervenuti su una Ford Ka) per raggiungere la porta digitale sul retro (ovviamente l'operazione dovrà essere fatta una sola volta!).
Sfiliamo il blocco autoradio.

▲ *Si tratta di arrivare alla porta digitale che sta sul retro dell'autoradio. Sulla Ka è abbastanza facile, sulle altre macchine dipende!*

Sul retro dell'autoradio vediamo la porta d'ingresso per il caricatore CD, che verrà collegata all'interfaccia AUX).
Colleghiamo il blocchetto dell'interfaccia AUX all'autoradio. Dopo il collegamento abbiamo deciso di far passare il cavetto sotto il posacenere davanti al cambio, in modo che sia in una posizione allo stesso tempo comoda per l'utilizzo e non d'intralcio. Dopo il montaggio l'interfaccia AUX scomparirà all'interno del cruscotto, dietro l'autoradio.

▲ *Nel cerchietto rosso si vede la porta che ci interessa.*

▲ *In questa foto possiamo vedere il cavetto con attacco minijack, che inseriremo nella presa cuffie dell'iPod, sbucare da sotto il cruscotto e il vano radio.*

Ora non rimarrà altro da fare che inserire il cavetto nell'iPod (consigliamo di farlo sempre con l'autoradio spenta) ed accendere la radio in modalità CD. Fatto! Che cosa suoniamo? Beh, quello che ci va. L'iPod è lì apposta!

▲ *iPod e autoradio, insieme!*

Le nostre impressioni sono complessivamente molto buone. Con l'interfaccia di Bortesi riusciamo ad ottenere un livello qualitativo molto elevato purché, ovviamente, gli MP3 (o gli altri formati supportati dal player) archiviati sul nostro iPod siano stati realizzati con un bit rate buono (almeno 192 kbps).
In definitiva, con una spesa esigua, e soprattutto senza dover cambiare autoradio, possiamo sfruttare iPod in auto senza sacrificare la qualità dell'ascolto.

Ghisa

Come un BIDONE

NESSUNO CI PENSA, ma da un disco rigido abbandonato nella spazzatura salta fuori di tutto, e il vicino di casa può andare a spiare nella spazzatura

▲ *Qualcuno potrebbe aprirlo, prendere il nostro disco rigido e frugarci dentro...*

In America gli hacker di una volta frugavano la notte nell'immondizia delle aziende in cerca di numeri di servizio da usare per chiamare gratis. Oggi le discariche contengono qualcosa di molto più prezioso: gli hard disk.

Qualche tempo fa Simson Garfinkel (http://simson.net/blog/), giornalista tecnico americano, ha svolto un'indagine, letteralmente, tra i rifiuti, andando a cercare dischi rigidi nella spazzatura, e poi comprando vecchi dischi usati nei mercatini rionali e nelle aste sul Web.
Dai dischi buttati via o comprati di seconda e terza mano ha ricavato più di cinquemila numeri di carta di credito, rapporti medici, informazioni familiari e finanziarie, nonché interi gigabyte di posta elettronica e file pornografici appartenenti ai precedenti proprietari dei dischi in questione.
Secondo Dataquest, nel 2001 sono andati fuori servizio più di 130 milioni di dischi rigidi in tutto il mondo, e 150 milioni nel 2002.

PROGRAMMI SPAZZATUTTO

Ecco alcuni programmi progettati per assicurare che i vecchi dati vengano distrutti per sempre:

- **CyberScrub**
  http://www.cyberscrub.com/
  A pagamento (39.95 dollari), demo 15 giorni
- **Data Scrubber Hard Drive Degaussing Software** http://www.datadev.com/ds100.html
  1.995 dollari!
- **Eraser**
  http://www.heidi.ie/eraser/
  Donateware (15 dollari)
- **UniShred Pro**
  http://www.lat.com/
  A pagamento (anche per Linux, 450 dollari)
- **WipeDrive**
  http://www.accessdata.com/Product07_Overview.htm39,95 dollari
- **Wipe:** http://wipe.sourceforge.net/
  Free, anche per Linux

della SPAZZATURA

SPROTETTI DALLA LEGGE

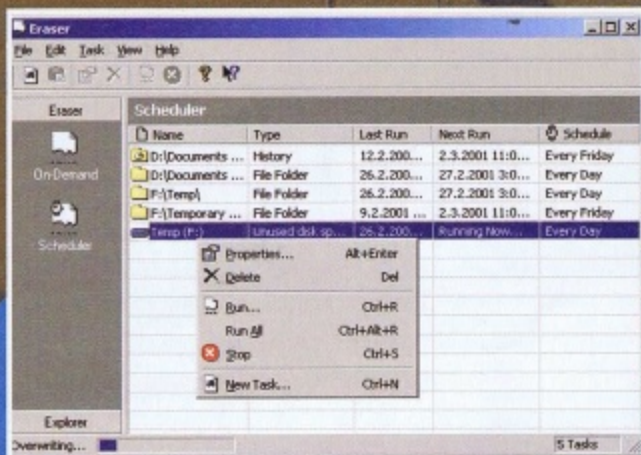
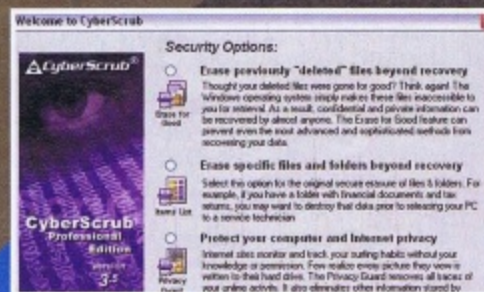
Ci sono casi e casi, ma in genere non vi è diritto alla privacy sui dati che vengono gettati nella spazzatura. Quindi chi andasse a frugare in un nostro vecchio hard disk potrebbe non correre rischi.

NO!

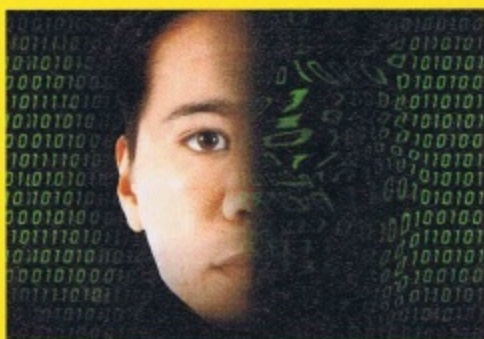
Avete cancellato i dati dal disco fisso del vostro vecchio PC prima di buttarlo?

Di 158 hard disk comprati in giro a prezzi ridicoli, 129 erano ancora funzionanti. 28 di questi conservavano i dati in chiaro, senza che nessuno si fosse preoccupato di cancellare qualcosa. In uno dei dischi c'era addirittura la registrazione di un anno di transazioni finanziarie: faceva parte di un vecchio bancomat.

Anche dove i dati erano stati cancellati, nella maggior parte dei casi un banale comando Undelete compiuto con programmi di riparazioni, tipo le Norton Utilities, ha riportato a galla una gran quantità di dati. La maggior parte delle persone pensa che basti cancellare un file per eliminarlo dalla faccia della terra; invece il file viene soltanto dimenticato dal computer, che considera scrivibile lo spazio da esso occupato, ma in effetti lo lascia dov'è. Di tutti i dischi, solo dodici erano stati adeguatamente ripuliti, senza che fosse possibile recuperare qualcosa. Nemmeno la riformattazione è un processo completamente sicuro. Le agenzie superprofessionali asseriscono di poter recuperare un file che è stato sovrascritto dalle testine del disco anche sette o otto volte.

Significa che, se vogliamo liberarci in modo veramente definitivo dei dati presenti sul nostro vecchio disco rigido, cancellarli o riformattare una volta sola non basterà. Una buona procedura consiste nel riformattare almeno dieci volte e poi distruggere fisicamente il disco, facendolo a pezzetti troppo piccoli perché sia possibile ricavarne qualcosa (se i pezzetti sono troppo grandi ci sono ancora possibilità!) È un paradosso; quante volte succede che sia fin troppo facile perdere dati preziosi? Eppure liberarsene per sempre, al 100 % di sicurezza, è assai più difficile.

▲ Eraser promette di cancellare completamente i dati sensibili ed è gratis. Anzi, chi lo usa viene esortato a pagare 15 dollari, nella logica del donateware.

▲ CyberScrub è uno dei numerosi tool che aiutano a distruggere definitivamente e in sicurezza i file confidenziali.

LADRI DI IDENTITÀ

Secondo uno studio commissionato dalla Federal Trade Commission americana, più di un americano su 25 ha subito nell'anno appena trascorso un furto di identità, da lieve – magari un abbonamento non voluto a un sito porno, effettuato da qualcuno che ha rubato un numero di carta di credito – a gravissimo, con la vera e propria appropriazione di un'identità da parte di un malintenzionato, negli ultimi cinque anni, è successo a un americano su dieci. Il danno economico si valuta su circa diecimila dollari per vittima, per un totale di 33 miliardi di dollari nell'ultimo anno. In Italia le cifre sono certamente inferiori, ma per nessuna delle vittime italiane è una consolazione particolare.

FACCIAMOCI

Can, in inglese, sta per scatola, barattolo. Un paio di connettori, un po' di inventiva, qualche spruzzo di teoria per sapere cosa fanno le onde radio quando viaggiano e siamo a posto: abbiamo costruito la nostra c-antenna

Un barattolo del caffé macinato, un connettore, uno spezzone di filo di rame grosso e un po' di pratica. Ecco come possiamo costruirci un'ottima antenna WiFi per migliorare la ricezione o puntare a trasmettitori più distanti.

Senza teoria

Il principio è abbastanza semplice. Se piazziamo un'antenna della giusta lunghezza dentro un barattolo del giusto diametro e la fissiamo bene alla distanza corretta dal fondo, è assicurata la risonanza con le onde radio che consentono il collegamento tra il trasmettitore e il nostro computer. Così riceveremo meglio e più di prima.
Il problema è quello di trovare le distanze giuste di tali pezzi e di mantenere un po' di precisione nel montaggio. Ma per fortuna non ha importanza conoscere la teoria delle antenne. Anche perché Internet viene in aiuto e un calcolatore apposito fa i conti per noi.

L'aspetto di un cavetto per collegare la cantenna al computer

I pezzi necessari

Procuriamoci un barattolo di dimensioni adeguate, diciamo circa 10 centimetri di diametro. Un barattolone del caffé macinato potrebbe andare bene, ma il divertimento è proprio questo: possiamo provare con diversi contenitori, i più disparati.
Procuriamoci anche un connettore di tipo N per il montaggio a pannello: lo possiamo trovare presso qualunque negozio che vende componenti elettronici (come per esempio http://www.marcucci.it/prodotti/schede/scheda.asp?ID=1935) e presso un ferramenta quattro viti con

UNA C-ANTENNA

dado che vadano bene per fissarlo.
Poi ci serve anche uno spezzone di filo di rame rigido numero 12 (lo chiediamo a un negozio di elettricisti) che taglieremo in modo che sia lungo circa 3,5 cm e che spelleremo in modo da lasciare solo il rame nudo.
Saldiamolo sul retro del connettore tipo N: questo sarà il nostro ricevitore d'antenna, che poi sistemeremo per bene.

La costruzione

Ora dobbiamo montare il connettore in modo che il ricevitore appena costruito si trovi all'interno del barattolo e alla distanza esatta dal fondo. Come si fa a calcolarla? Semplice. Prima dividiamo per 2,54 il diametro in centimetri del barattolo. Per esempio, se il barattolo ha un diametro di 10 cm, gli equivalenti pollici sono circa 3,9.
Quindi andiamo all'indirizzo http://www.turnpoint.net/wireless/cantennahowto.html (da cui abbiamo tratto ispirazione e che potrà esserci utile) e, a circa metà pagina, troviamo un calcolatore dove inseriamo il valore appena scoperto.

3.9 **Can Diameter** Calculate

Cuttoff Frequency in MHz for TE11 mode	1773.66	MHz
Cuttoff Frequency in Mhz for TM01 mode	2316.63	MHz
Guide Wavelength in Inches	7.06	inches
1/4 Guide Wavelength	1.77	inches
3/4 Guide Wavelength	5.3	inches

▲ *Il calcolatore per costruire bene l'antenna... in scatola*

Un click su Calculate e otteniamo:
- la frequenza di taglio inferiore, sotto la quale l'antenna non servirà a nulla. Dovrebbe essere inferiore a 2.412 GHz
- la frequenza di taglio superiore, sopra la quale l'antenna non servirà a nulla. Dovrebbe risultare superiore a 2.462 GHz
- la distanza esatta a cui dovremo montare il ricevitore a partire dal fondo del barattolo, nel caso volessimo costruire un'antenna a _ d'onda

▲ *Un possibile barattolo e il connettore da pannello tipo N.*

Se le frequenze di taglio inferiore e superiore sono, più o meno, dentro i valori detti, annotiamo la distanza equivalente a _ dell'onda. Prendiamo il barattolo e, con precisione, misuriamo dal fondo chiuso tale distanza, facendo un segno sul barattolo. Lì dobbiamo fare un forellino, prima piccolo per esempio con un chiodo o una punta da trapano sottile, e poi eventualmente più grande in modo che il filo di rame che abbiamo saldato al connettore non tocchi il metallo del barattolo.
Dopodiché dobbiamo, con attenzione, segnare sul barattolo anche la posizione delle viti che terranno fermo il connettore e fare i relativi buchi. Teniamo la testa delle viti dentro il barattolo e i dadi fuori, così ostacoliamo il meno possibile la nostra antenna.
Non stringiamo i dadi, perché dobbiamo ancora rifinire l'antenna. Infatti è necessario regolare lo spezzone di rame rigido, che ora sporge dentro il barattolo, in modo che la lunghezza complessiva a partire dalla parete del barattolo sia il più possibile vicina a 3 cm. Segniamolo con un pennarello, estraiamo il connettore svitandolo, tagliamo esattamente dove c'è il segno e rimontiamo il tutto. È fatta! Un cavetto RU 58 e qualche connettore per il collegamento alla scheda WiFi del computer e potremo verificarne il funzionamento. Un'ultima curiosità: questo tipo di antenne sono polarizzate, quindi facendole ruotare cambia la resa. Sperimentiamo il tutto, ruotando, e con barattoli diversi...

Standard Bus
standardbus@softhome.net

COSA SONO LE ANTENNE?

Immaginiamoci di essere su un ponte sopra un fiume. Sotto passa una barca a remi. Le onde vanno a sbattere contro i piloni del ponte. Appoggiamo l'orecchio al ponte: sentiamo amplificato il suono delle vibrazioni che le onde generate del battello trasmettono ai piloni. Uno sciabordio lento e cadenzato: a una frequenza piuttosto bassa, perché la lunghezza tra le singole onde è piuttosto grande. Bene, ci siamo: se trasportiamo questo esempio alle onde radio, il periodo che passa tra un'onda e l'altra è molto più piccolo. Per le onde radio che usiamo nel Wi-Fi, e in particolare in quello standard che chiamiamo 802.11b, le onde si ripetono 2.400.000.000 volte in un secondo. Cioè, in altre parole, hanno una frequenza di 2,4 GigaHertz. Che cos'è il ponte? La nostra antenna, naturalmente! Quello che fa l'antenna è acchiappare queste onde che viaggiano nell'aria, come fa una vela con il vento. E come per una vela, possiamo usare qualunque cosa per costruire un'antenna. Dopodiché funzionerà più o meno bene: meglio se si accorderà al tipo, alla quantità e alla direzione del vento. Se qualche pezzo metallico dell'antenna sarà in una dimensione pari alla lunghezza dell'onda in arrivo, entrerà in risonanza e così avremo in uscita una corrente elettrica più forte. Funziona anche se è un multiplo o una frazione della lunghezza d'onda che vogliamo catturare. Antenne da un quarto della lunghezza d'onda, per esempio, sono molto comuni.

LYX batte WORD

Le cose da sapere per installare LyX e per usarlo al meglio come potente tritadocumenti

LyX nasce nel mondo Unix ma può essere usato su qualsiasi computer, Windows, Linux o Mac OS X. I più bravi possono scaricare il sorgente e compilarlo sulla propria macchina; per il resto di noi, esistono eseguibili già pronti all'uso.

Per Windows si trova un porting nativo di LyX a http://www.home.zonnet.nl/rareitsma/lyx/. Su questa pagina si trovano tutti i link necessari per avere LyX up and running, attivo e funzionante. Un'altra pagina buona è http://wwwserv1.rz.fh-hannover.de/mbau/tim/hentschel/lyx/index.htm, anche se sembra un po' meno aggiornata. Quasi certamente sarà necessario installare Cygwin, reperibile a http://www.cygwin.com/.

Per Mac OS X tutte le istruzioni, e i link giusti, si trovano a http://www.18james.com/lyx_on_aqua.html. Il fatto che Mac OS X sia Unix facilita le cose rispetto a Windows.

Fraction
Square root
Exponent
Index
Sum
Integral
Math mode
Display
Math Panel...

◄ *LaTeX - e LyX - è inarrivabile nel trattamento delle formule matematiche. Per inserirne una scegliamo Math Mode dal menu Math di LyX. Nell'editor appare un riquadro blu in cui troverà posto la formula. I simboli matematici si inseriscono da una palette piuttosto semplice.*

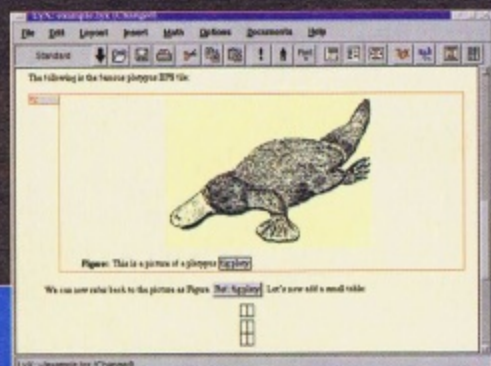
Per Linux non c'è problema. Le distribuzioni come RedHat o Debian comprendono già il pacchetto, pronto da usare. A ftp://ftp.lyx.org/pub/lyx/ si trovano comunque gli RPM più aggiornati.

Per tutti è indispensabile avere una versione di TeX (LaTeX, teTeX, OzTeX eccetera) preinstallata. LyX è un bellissimo quadro comandi, ma senza il motore sottostante non può funzionare. Il motore è TeX. Per il mondo Unix un indirizzo possibile è http://www.tug.org/teTeX/; per Windows

LYX A LATEX

due delle numerose pagine possibili sono http://www.princeton.edu/~gchouse/tex.html e http://miktex.org/.

Con chi parlare

Esistono diverse risorse, da mailing list a newsgroup a canali di chat, dedicati a chi usa LyX. Per essere al

▲ *Per inserire una tabella selezioniamo Insert -> Table e specifichiamo il numero di righe (Rows) e colonne (Columns). Nell'editor appare una griglia corrispondente alle nostre indicazioni. Per riempire la tabella basta scriverci dentro. Si passa da una casella all'altra con il mouse o con i tasti cursore. Presa l'abitudine, lavorare con LyX è davvero molto rapido. E i risultati sono ottimi.*

corrente degli aggiornamenti di LyX basta iscriversi alla mailing list dedicata, che ha volume di traffico molto basso. Gli indirizzi da conoscere sono tre, basta inviare una mail vuota:

- lyx-announce-subscribe@lists.lyx.org per iscriversi
- lyx-announce-unsubscribe@lists.lyx.org per disiscriversi
- lyx-announce-help@lists.lyx.org per ricevere un messaggio di istruzioni

Esiste naturalmente una lista di utenti, dove si fanno domande e sperabilmente si ricevono risposte. L'indirizzo della lista è lyx-users@lists.lyx.org. Per gestire la lista (basta un messaggio vuoto) scriveremo a:

- lyx-users-subscribe@lists.lyx.org per iscriversi
- lyx-users-unsubscribe@lists.lyx.org per disiscriversi
- lyx-users-help@lists.lyx.org per ricevere un messaggio di istruzioni

Quando si trattano formule matematiche LyX lascia Word nella polvere

Per sviluppatori e programmatori la lista è lyx-devel@lists.lyx.org e i messaggi di gestione... beh, un programmatore può leggere qui sopra e capire a che indirizzo iscriversi o disiscriversi!Sono disponibili varie altre mailing list più specifiche all'indirizzo http://www.lyx.org/ internet/mailing.php3.

Trucchi e consigli

All'indirizzo http://latex.s-v-p.de/ si trova un elenco molto ricco di trucchi e consigli per raggiungere risultati specifici con LaTeX, dagli accorgimenti per la generazione di file Pdf a come disegnare un circoletto intorno a una lettera (qualcuno ha mai provato a farlo con Word?). Nei prossimi numeri di Hacker Journal entreremo nei dettagli dell'installazione di LyX e dell'uso del programma. Come al solito, basta chiedere... e risponderemo!

Barg the Gnoll
gnoll@hackerjournal.it

HO SOLO UN MODEM 56K!

Hackers Magazine numero 17, in edicola proprio in questi giorni, contiene nel CD una versione completa di LyX, che permette di evitare di doversi scaricare il software con una connessione lenta.

BASTA CANONI

◄ *L'incubo della voce su Internet è la packet loss, la perdita dei pacchetti. Se sono troppi, o se si perdono quelli critici, la comunicazione ne risente.*

Dopo avere parlato delle sue basi in Hacker Journal 45, è tempo di scendere nelle viscere del protocollo VoIP per parlare a viva voce attraverso Internet. VoIP significa Voice over IP ed è il sistema di regole che permette di far viaggiare la viva voce sui cavi di rete e, per esempio, telefonare legalmente senza dover pagare alcun canone. La voce viene convertita da analogica a digitale, prima di andare su Internet, e al termine del viaggio viene convertita da digitale ad analogica. Per ridurre il peso dei dati viene compressa in partenza e decompressa all'arrivo.

Qualsiasi scheda audio contenuta in un computer consente di convertire con 16 bit, cioè due byte, una banda di 22.050 hertz a una frequenza di campionamento di 44.100 hertz. ne risulta un flusso di dati di 2 byte * 44.100 hertz = 88.200 byte. Tutto ciò accade ogni secondo ed equivale a circa 176,4 KB per secondo. Le esigenze di VoIP sono largamente inferiori a queste. Gli algoritmi di compressione della voce per fare Voice over IP sono vari.

RTP fornisce funzioni di trasporto su rete da punto a punto adatte per applicazioni di trasmissioni di dati in tempo reale, come audio, video o simulazioni, su servizi di rete multicast o unicast

PCM, Pulse Code Modulation

PCM prevede una banda voce di 4 kHz e quindi un campionamento di 8 kHz. Ogni campione viene rappresentato con otto bit (quindi 256 valori possibili), il che porta a un throughput (flusso di dati) di 8.000 hertz * 8 bit = 64 kbit per secondo (kbps), che è la misura tipica della linea telefonica digitale.

ADPCM, Adaptive Differential PCM

Questo algoritmo lavora sulla differenza tra la voce appena pervenuta e quella in arrivo, riducendo la banda necessaria a 32 kbps.

LPC-10

Sembra incredibile, ma LPC-10 riesce a raggiungere una fedeltà molto alta con bande ridottissime, anche 2,5 kbps! Il prezzo da pagare, però, è una elaborazione pesantissima, che di fatto può quasi paralizzare un computer.

Altri algoritmi

Oltre alle scelte citate abbiamo altre sigle come LD-CELP, CS-ACELP, MP-

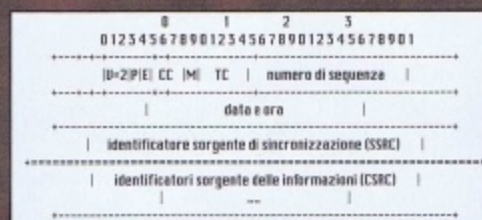
alle compagnie TELEFONICHE

MLQ e ACELP, che si situano tra gli estremi di PCM e LPC-10. Sono da notare MP-MLQ e ACELP, rispettivamente con bande di 6,3 e 5,3 kbps.

RTP, Realtime Transport Protocol

Perché i dati della voce possano viaggiare su Internet via IP è necessario incapsularli nello stack TCP/IP. È una specie di matrioska, un'informazione dentro l'altra: i pacchetti dati di voce VoIP stanno dentro pacchetti RTP, che a loro volta sono contenuti in pacchetti UDP-IP. Scopriamo che in fin dei conti VoIP non usa TCP, perché troppo pesante per applicazioni di trasmissione dati in tempo reale, ma UDP. Quest'ultimo è abbastanza leggero per il lavoro da compiere ma ha un altro difetto: non controlla l'ordine in cui arrivano i pacchetti né il tempo che ci mettono. In concreto, la voce viene mandata su Internet frammentata in tanti spezzoni, ma ognuno di essi può prendere una strada diversa dagli altri e metterci più o meno tempo. Se i pacchetti non arrivano abbastanza in fretta da essere ordinati e non lasciare troppi buchi, la ricezione è un disastro. A questo pensa RTP, che può decidere quando i dati sono abbastanza completi da non attendere troppo un pacchetto perso per strada. Non è importante che arrivino tutti e insieme, ma che arrivino in quantità sufficiente, in continuazione e il più possibile ordinati.

Un pacchetto RTP (Realtime Transport Protocol), usato per trasportare la voce su Internet.

```
        0                   1                   2                   3
        0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
       +-+-+-+-+-------+-+-------------+-------------------------------+
       |V=2|P|E|  CC   |M|     TC      |      numero di sequenza       |
       +-+-+-+-+-------+-+-------------+-------------------------------+
       |                           data e ora                          |
       +---------------------------------------------------------------+
       |      identificatore sorgente di sincronizzazione (SSRC)       |
       +===============================================================+
       |      identificatori sorgente delle informazioni (CSRC)        |
       |                              ...                              |
       +---------------------------------------------------------------+
```

V = versione di RTP usata
P = byte di padding, presente solo per fare numero e raggiungere i 32 byte
E = estensione header
CC = numero di identificatori della sorgente delle informazioni (CSRC) che seguono l'header fisso
M = bit marker
TC = tipo di carico

In un prossimo articolo proseguiremo a parlare dei componenti di Voice over IP, a partire dal protocollo RSVP che sembra un invito a cena ufficiale e invece assicura una cosa assai importante: la Quality of Service, o QoS.

Nyarlathotep
nyarlathotep@hackerjournal.it

Chi trova la soluzione ottimale per telefonare via internet può davvero fare una barca di soldi

TUTTE le foto

Con un linguaggio potente e flessibile quale PHP possiamo fare molto, compreso gestire un album fotografico sul Web

Scattare foto digitali è così facile che condividerle e mostrarle a chi vuole non dovrebbe essere complicato. Ecco come pubblicarle sul Web con un po' di PHP fatto come si deve.

Prima di tutto ottimizziamo i nomi dei file, cosa che facilita la programmazione. La cosa migliore è scegliere una convenzione, per esempio foto1.jpg, foto2,jpg, foto3.jpg eccetera, in cui il nome resta identico tranne per un numero che si incrementa.

Poi passiamo a realizzare la pagina Web, con un misto di HTML e PHP:

```
<?php

//specifichiamo il percorso (path) allo script
//(per esempio /var/www/html/albumfoto.php)
```

Abbiamo un nucleo che consente di mostrare immagini una dopo l'altra

```
$percorso = getenv("NOME_SCRIPT");

//prendiamo la directory dello script
//(per esempio /var/www/html)
$dir = dirname($percorso);

//percorso relativo alle foto
$percorso_foto = "/immagini/foto";

//combiniamo le due variabili per creare il percorso completo
$dir .= $percorso_foto;

//proviamo ad aprire la cartella che contiene le foto
if ($handle = opendir($dir)) {

  //impostiamo un conteggio
  $conto_file = 0;

  //ora usiamo la funzione "readdir" per contare i file nella cartella
      while (false !== ($file = readdir($handle))) {
      ++$conto_file;
  }

  //chiudiamo la directory
  closedir($handle);

  //escludiamo dal conteggio i file
```

in RETE

```
che non sono foto;
  //molti server contengono file
come "." e ".."
  $conto_file = $conto_file-2;


  //impostiamo il numero della foto
corrente
  //e creiamo la variabile relativa
al suo nome

  //se la foto non è stata inviata via
URL,
  //usiamo la variabile conto_file
  if($numero_foto == ''){
    $numero_foto = $conto_file;
  }

  //creiamo il nome della foto, per
esempio foto1.jpg
   $foto = "foto" . $numero_foto .
".jpg";

}

//se opendir non riesce, segnalia-
mo l'errore
else{
  echo("ERRORE IN LETTURA DI $dir");
}

?>
```

A questo punto abbiamo impostato due variabili, necessarie per mostrare la foto corrente, possibilmente con link per andare avanti e indietro. La variabile $foto conterrà il nome della foto corrente e la variabile $conto_file contiene il numero totale delle foto dentro l'album.

Il codice seguente mostra la foto e i link avanti-indietro:

```
<?php

//leggiamo gli attributi dell'imma-
gine
//usiamo la variabile $dir definita in
precedenza

list($larga, $alta, $tipo, $attr) =
getimagesize("$dir/$foto");


//visualizziamo l'immagine
?>

<img                    src="<?
echo("$percorso_foto/$foto"); ?>"
width="<?  echo($larga);  ?>"
height="<? echo($alta); ?>" bor-
der="2">

<?php
  //confrontiamo numero_foto con
la variabile conto_file
  //se si equivalgono, il link Indie-
tro non deve apparire
  //perché siamo all'inizio

  if($numero_foto != $conto_file){

    $prec_foto = $numero_foto + 1;
?>

<                                a
href="albumfoto.php?numero_foto
=<?   print($prec_foto);   ?>"
class="piclink"><- Indietro</a> ::::

 <?php
  }

  //controlliamo se siamo all'ulti-
ma foto.
  //se sì, il link Avanti non deve
apparire.

  if($numero_foto != 1){

    $prox_foto = $numero_foto - 1;
?>

<                                a
href="albumfoto.php?numero_foto
=<?   print($prox_foto);   ?>"
class="piclink">Avanti -></a><br>

<?php
  }
?>
```

Chiaramente questo è solo l'inizio, ma abbiamo il nucleo di un programma che consente di mostrare immagini una dopo l'altra in un album fotografico su Web.

Le possibilità a disposizione sono infinite. Per esempio mostrare più miniature cliccabili in una singola pagina. Dovrebbero stare in una cartella miniature che sta accanto alla cartella foto, e il programma visualizzerebbe le miniature, ognuna linkata alla foto a grandezza reale. Oppure, più interessante come programmazione, si potrebbe usare la funzione rand() per creare un pulsante a caso che mostra una foto scelta casualmente tra tutte quelle a disposizione. Chi è capace di arricchire ulteriormente questo codice? Attendiamo risposte!

Nyarlathotep
nyarlathotep@hackerjournal.it

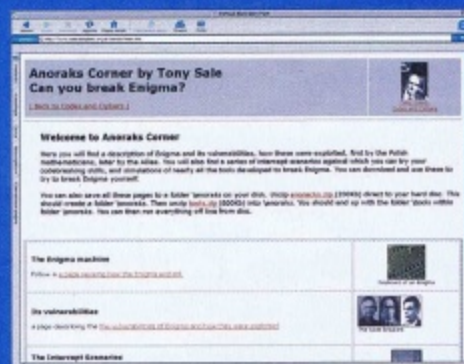
CODICE NAZISTA:

La macchina che generava i codici segreti per i nazisti nella Seconda guerra mondiale

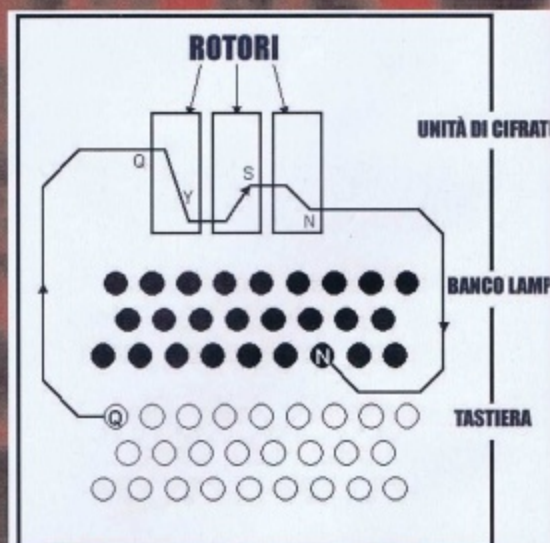
CHI È CAPACE DI VIOLARE ENIGMA?

All'indirizzo http://www.codesandciphers. org.uk/anoraks/index.htm si trovano tutte le informazioni utili, le simulazioni di macchine Enigma autentiche e gli strumenti informatici del mestiere per arrivare a violare il codice della macchina. Chi ama le sfide troverà pane per i suoi denti. Roba del secolo scorso, ma tosta.

Anoraks Corner by Tony Sale
Can you break Enigma?

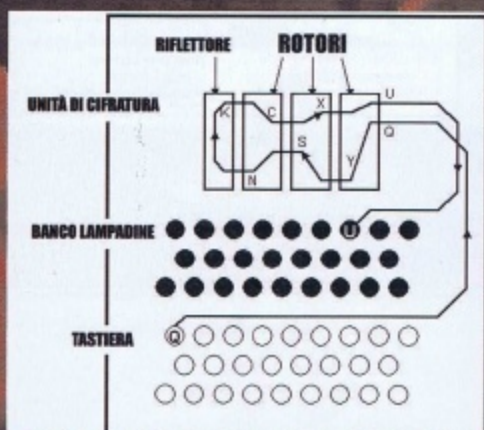
Welcome to Anoraks Corner

Pochi sanno che Enigma nacque nel 1923 a scopo commerciale, destinata alle aziende con esigenze di confidenzialità, a opera di tale Arthur Scherbius. Il suo funzionamento doveva essere semplicissimo: un operatore digitava una lettera in chiaro e si accendeva una lampadina che indicava la lettera in testo cifrato. Bastava prendere nota delle lettere cifrate per costruire il messaggio. In realtà questa prima versione non fu costruita.

Ogni lettera premuta attivava un circuito specifico, che passava tensione a uno dei 26 contatti presenti nell'unità di cifratura. Da lì il segnale attraversava tre rotori, ognuno dei quali cambiava la lettera che gli arrivava in un'altra. Dopo ogni lettera il primo rotore avanzava di una posizione; dopo 26 lettere il secondo rotore avanzava di una posizione e dopo 676 lettere avanzava di una posizione anche il terzo rotore. Questo faceva sì che in un messaggio di lunghezza normale sarebbe stato

ROTORI
UNITÀ DI CIFRATU
BANCO LAMP
TASTIERA

▲ *Il primo progetto di Enigma. La freccia indica il percorso dell'informazione e della cifratura della lettera. La meccanica di cifratura cambia dopo ogni tasto premuto.*

semplice ed efficace

impossibile avere due lettere cifrate nella stessa maniera.

Enigma doveva essere facile da usare, ma questo progetto rendeva difficile l'ingegnerizzazione della decodifica. Così si invertì la sequenza dei rotori e venne aggiunto in fondo allo schema un rotore di riflessione, che rimandava il segnale dentro i rotori stessi. Enigma venne costruita con questo progetto. Una soluzione semplice ed elegante che però conteneva un grave difetto. Il rotore di riflessione implicava che nessuna lettera poteva mai essere codificata in se stessa.

▲ *Il progetto di Enigma usato dall'esercito tedesco, con l'aggiunta di un riflettore al termine della sequenza di rotori. In seguito vennero aggiunti altri due rotori.*

Dal commerciale al militare

L'esercito tedesco mise subito gli occhi su Enigma, che venne ritirata dal commercio e complicata da un meccanismo aggiuntivo, detto Stecker, che scambiava coppie di lettere tra loro. I tedeschi continuarono a lavorarci sopra e prima aggiunsero altri due rotori facoltativi, che permettevano di scegliere tre rotori dai cinque disponibili, e poi si arrivò – nel 1942 – all'introduzione di un quarto rotore effettivo, che rafforzava molto la cifratura. Rimaneva però la falla che contribuirà alla decifrazione e alla sconfitta bellica.

Falsa sicurezza

I tedeschi pensavano che Enigma fosse inviolabile. Sbagliavano. I primi a vedersela con il suo cifrario furono i polacchi, quando per errore la Germania inviò a un proprio diplomatico a Varsavia un dispaccio Enigma per posta ordinaria. Le insistenti richieste tedesche di riavere il pacco insospettirono i doganieri polacchi, che per un fine settimana esaminarono il messaggio prima di richiuderlo e reinviarlo al mittente.

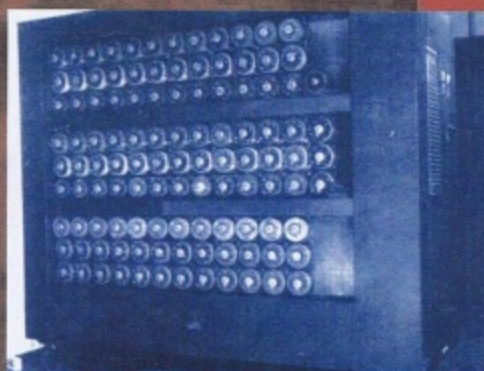
La sicurezza di Enigma non stava nel modo in cui è costruita la macchina, ma nell'enorme numero di stati diversi in cui poteva trovarsi, dalla diversa disposizione dei rotori alla loro posizione iniziale fino alle connessioni dello Stecker. Ma c'erano punti deboli. Oltre alla falla già descritta, per esempio, si chiedeva agli operatori della macchina di iniziare ogni messaggio trasmettendo due volte di seguito le tre lettere corrispondenti alla posizione iniziale dei rotori. Per i crittanalisti fu un vero regalo.

A caccia di femmine

La femmina è una situazione in cui due lettere conosciute (per via della ripetizione iniziale) venivano cifrate nella stessa lettera. I polacchi costruirono una macchina, detta bomba, con circuiteria simile a quella di Enigma, che poteva tenere conto delle femmine e cercare di farle corrispondere a tutte le possibile posizioni dei rotori fino a che non trovava quella giusta. Serviva una bomba per ogni ordinamento dei rotori e quindi, con tre rotori, servivano sei bomba. Enigma tornò sicura nel dicembre 1938, quando vennero inseriti altri due rotori. I polacchi non potevano costruire sessanta bomba. Stava arrivando il momento degli inglesi.

Il Turing club

Nel gennaio 1939 a seguito di un incontro tra spionaggio polacco, francese e inglese, andò all'attacco di Enigma la British Government Code & Cypher School, con l'ausilio di uno dei più grandi matematici di tutti i tempi, Alan Turing. Gli inglesi costruirono le sessanta bomba necessarie e andarono oltre, con una nuova versione detta Bombe.

La Bombe era più svelta e intelligente, capace di applicare criteri di probabilità ai messaggi cifrati. Infatti, contrariamente alle specifiche del governo tedesco, spesso i messaggi Enigma iniziavano con le stesse parole. Le nuove possibilità della Bombe

▲ *La Bombe, macchina usata dagli inglesi per decifrare Enigma, cui contribuirono i servizi segreti polacchi e il celebre matematico Alan Turing. Pesava una tonnellata.*

e le debolezze intrinseche di Enigma furono abbastanza per violare il codice e contribuire alla sconfitta di Hitler.
Non fu cosa da niente, comunque; alla fine della Seconda guerra mondiale presso Bletchey Park, sede degli sforzi di decrittazione inglesi, lavoravano a turni 24 ore su 24 oltre diecimila persone!

Kurt Gödel
kurtgoedel@hackerjournal.it

Il TETRIS più

Sembra una barzelletta: che cosa fanno un computer Linux, una rete dati estesa per dodici piani, un radiocontroller per giochi, undici schede di circuiti costruite a mano e diecimila luci di Natale? Il Tetris più grande del mondo, ovvio!

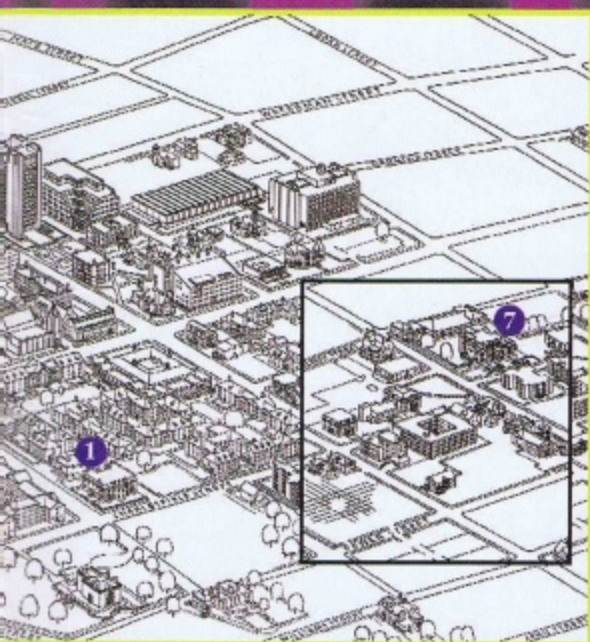
Si chiama La Bastille ed è stata realizzata con un lavoro di cinque mesi dalla community universitaria Technology House (http://techhouse.brown.edu/) presso la Brown University (http://www.brown. edu/) di Providence, nel Rhode Island, non lontano da New York. Più esattamente, dal 14 al 22 aprile del 2000 la Biblioteca delle Scienze dell'università è stata trasformata nel più grande Tetris del mondo, che si poteva vedere in funzione a chilometri di distanza.

Il progetto sfruttava l'altezza dell'edificio e le sue numerose finestre, trasformate in giganteschi pixel dall'installazione di migliaia di lampadine natalizie, che il computer provvedeva ad accendere e spegnere per rendere agli osservatori dall'esterno l'impressione dei blocchi che cadono e ruotano, come nel gioco originale. Al progetto ha lavorato direttamente una squadra di oltre trenta persone, che hanno dedicato al progetto i loro fine settimana liberi.

▲ La pianta della Brown University. La Bastille, il Tetris più grande mai giocato, è stato installato nell'edificio numero 8, a Science Library

Poteva essere visto in funzione da svariati chilometri di distanza. Oggi è un reperto da museo ma resta interessante scoprire come era fatto

Il controller via radio appositamente realizzato per controllare il mega Tetris

grande del MONDO

Si poteva vederla in tre modi. Come un omaggio ai videogiochi, come una sfida hardware o come un grande hack.

Keith Dreibelbis, animatore del progetto

Le luminarie natalizie sono state installate su telai di legno ricavati da vecchi pallet e la cablatura dell'installazione – che funziona regolarmente nelle ore diurne come biblioteca – ha sfruttato spazi improvvisati come un vecchio passavivande in disuso che attraversava verticalmente l'edificio.
Per giocare è stato messo a punto un controller wireless adattato a partire da una console Super Nintendo, che consentiva di pilotare il gigantesco Tetris a una distanza anche di un centinaio di metri.
Durante il lavoro l'ascensore di servizio è stato attivato 12.347.065 volte per organizzare l'hardware disposto sui tredici piani dell'edificio. I partecipanti al progetto erano organizzati con walkie-talkie per comunicare ovunque, anche nell'oscurità dei passaggi in cui passava la spina dorsale del cablaggio. È stato effettuato un numero praticamente incalcolabile di saldature e connessioni, tale da mettere statisticamente a rischio il funzionamento stesso dell'installazione.

Il 27 maggio 2000 centinaia di studenti e personale della Brown University poterono usare La Bastille per l'ultima volta, prima che venisse smontata e messa in magazzino. Da allora si aspetta che qualcuno osi organizzare qualcosa di più grande. Chi sarà il prossimo?

Reed Wright
reedwright@mail.inet.it

Il Tetris in funzione attraverso le finestre della Science Library. Si vede bene, in alto, un pezzo zig-zag in caduta.

RIPROVIAMOCI IN JAVA

Anche se La Bastille non esiste più è stato realizzato un suo simulatore in Java, reperibile a http://bastilleweb.techhouse.org/applet/. Fa impressione!

HACKER JOURNAL

IL PROSSIMO NUMERO
IN EDICOLA
IL 8 APRILE 2004!

??? CYBERENIGMA ???

Una sfida tira l'altra! Ecco pane per i nostri denti. Facciamo funzionare le meningi oppure, a scelta, rotoliamo la pallina del mouse a caccia di siti con gli strumenti giusti per una rapida soluzione. Questa volta è un assaggino, un antipasto, uno stuzzichino. Iniziamo dalla parte semplice di un argomento difficile. Ma nelle prossime puntate la sfida diventerà sempre più esaltante!

Sommergeteci di soluzioni all'indirizzo: guestbook@hackerjournal.it

Pvsenevb qv Prfner

Genggb qn: Jvxvcrqvn, y\'rapvpybcrqvn yvoren. Qrggb napur \"rpprffb 3\" è vy cvù nagvpb nytbevgzb pevggbtensvpb qv phv fv noovn genppvn fgbevpn. va ernygà ha fbggbpnfb qv pvsenevb n fpbeevzragb qbir yn pvvnir nffhzr vy inybe svffb 3. Irqv napur EBG-13: vy pnfb pba pvvnir pba inybe 13.

Vy pvsenevb qv Prfner cerirqr pur nq btav yrggren iratn fbfgvghvgn yn gremn yrggren fhp-prffvin, hgvyvmmn dhvaqv yn frthragr gnoryyn qv pbairefvbar:

Bevtvanyr: nopqrstuvyzabcdefghim
Pevggngb: QRSTUVYZABCDEFGHIMNOP

Rppb snpvyzragr pnypbynovyr ha rfrzcvb qv grfgb:

Bevtvanyr: nggnppner tyv veevqhpvovyv tnyyv nyyn ben frfgn
Pevggngb: QMMQSSQHU YBA AHHATNSARABA YQBBA QBBQ EHQ IUIMQ

Pbzr fv chò snpvyzragr vaghver napur framn nyphan pbabfpramn qv pevggnanyvfv dhrfgb gvcb qv pvsenghen aba bsser nypha gvcb qv fvphermmn bttvtvbeab, shamvbanin nv grzcv qv Prfner fbyb cre y\'vaperqvovyr abivgà qryy\'vqrn va fé.

LA SOLUZIONE?
All'uscita del prossimo numero, la troverete nella secret Zone del sito www.hackerjournal.it